NORTH-HOLLAND

Fourier Transform Imitations

Ron Aharoni*
Technion
Haifa, Israel

Milton Maritz*
University of Bloemfontain
South Africa

and

Roy Meshulam†
Technion
Haifa, Israel

Submitted by Richard A. Brualdi

ABSTRACT

We consider a family of transforms which are generalizations of the Fourier transform on abelian groups. When the group under consideration is $\mathbb{Z}_n$, members of this family are characterized by having a matrix whose i,jth element is $a(ij \bmod n)$, where a is any given vector. We address the problem of when the inverse of a member of the family belongs to the family. © Elsevier Science Inc., 1997

*The work of the first two authors was supported by NIH grant HL28438, while visiting MIPG, Radiology Department, University of Pennsylvania.

†The work of the third author was supported by a grant from the fund for the promotion of research at the Technion.

655 Avenue of the Americas, New York, NY 10010

0024-3795/97/$17.00
PII S0024-3795(96)00153-X

1. WRAPPING MATRICES

In this section we shall define a special class of transforms over the group $\mathbb{Z}_n$. We shall later generalize this concept to general abelian groups, and re-prove the results in the general setting. However, we feel that it is valuable to see and prove first the case of $\mathbb{Z}_n$, in which the concept has a more concrete form. For an abelian group G we denote by $L(G)$ the linear space of complex valued functions on G. For a given function $a \in L(\mathbb{Z}_n)$ let $w(a)$ be the matrix whose i, jth element is $a(ij)$ (where i and j are elements of $\mathbb{Z}_n$, and their product is taken in $\mathbb{Z}_n$). A matrix of this form is called *wrapping*. Denoting by f the vector whose kth component is $e_n(k)$, where $e_n(k)$ is $\exp(2k\pi i/n)$, the matrix $w(f)$ is that of the Fourier transform. The main problem with which we shall be concerned is when the inverse of a wrapping matrix is also wrapping.

We do not know of any previous investigation of what are called here "wrapping matrices." However, similar notions have been studied for matrices whose indices belong to a group, rather than to the ring $\mathbb{Z}_n$. See for example the survey paper [3] and its many references.

The ith row of a matrix A is denoted by $A_{(i)}$, and the jth column by $A^{(j)}$. For $i \in \mathbb{Z}_n$ denote by Q_i the matrix whose k, jth element is 1 if $j = ki$ and is 0 otherwise. Denote by $\mathscr{Q}$ the subalgebra of $M_n(\mathbb{C})$ spanned by the matrices Q_i, $i \in \mathbb{Z}_n$. Clearly, $Q_i Q_j = Q_{ij}$, which implies that the elements of $\mathscr{Q}$ commute with each other. Let $\mathscr{R}$ denote the subalgebra of $\mathscr{Q}$ spanned by the matrices Q_i, $i \in \mathbb{Z}_n^*$, where $\mathbb{Z}_n^*$ is the set of all elements in $\mathbb{Z}_n$ which are coprime to n. Also let $\mathscr{P}$ be the subalgebra of $\mathscr{Q}$ spanned by the matrices Q_i, $i \notin \mathbb{Z}_n^*$.

For $i \in \mathbb{Z}_n^*$ one has

$$Q_i^{-1} = Q_i^T = Q_{i^{-1}}, \tag{1}$$

which implies:

LEMMA 1.1. *If $R \in \mathscr{R}$ then $R^T \in \mathscr{R}$.*

COROLLARY 1.2. *If $R \in \mathscr{R}$ and $Q \in \mathscr{Q}$ then $RQ^T = Q^T R$.*

Clearly, a matrix A is wrapping if and only if $A(ki, j) = A(i, kj)$ for all i, j, and k. In terms of the matrices Q_k, this means that $Q_k A = AQ_k^T$ for all k.

Let us write this as a lemma:

LEMMA 1.3. *A matrix A is wrapping if and only if $QA = AQ^T$ for all $Q \in \mathscr{Q}$.*

Lemmas 1.1 and 1.3 imply:

LEMMA 1.4. *If W is wrapping then $R^T W = WR$ for all $R \in \mathscr{R}$.*

Note that the ith row of $w(a)$ is equal to $Q_i a$. This implies:

LEMMA 1.5. *For each vector a and $Q \in \mathscr{Q}$ there holds $w(Qa) = Qw(a)$ (that is, w is a homomorphism of $M_n(\mathbb{C})$ as a module over $\mathscr{Q}$).*

If a and b are vectors such that $a = w(b)x$ for some vector x, then by the lemma $w(a) = w(\Sigma_{i \in \mathbb{Z}_n} x_i Q_i(b)) = \Sigma_{i \in \mathbb{Z}_n} x_i Q_i w(b)$, which yields:

COROLLARY 1.6. *If W is wrapping and $a = Wx$, then $w(a) = \Sigma x_i Q_i W$.*

We shall call a function v in $L(\mathbb{Z}_n)$ *periodic* if, for some proper divisor d of n (where "proper" means that $d < n$), $v(i + d) = v(i)$ for all $i \in \mathbb{Z}_n$. The subspace of $L(\mathbb{Z}_n)$ spanned by all periodic vectors is denoted by V_n. The space orthogonal to V_n will be denoted by U_n. Vectors in U_n are called coperiodic. Note that u is periodic if and only if u is in the image space of some matrix $P \in \mathscr{P}$. A vector u is coperiodic if

$$\sum_{k \in \mathbb{Z}_n} u(h + dk) = 0 \tag{2}$$

for all $h \in \mathbb{Z}_n$ and all proper divisors d of n. Of course, it suffices to require (2) to hold only for $d = n/p$ for prime divisors p of n.

LEMMA 1.7. *If $W = w(a)$ is nonsingular and $w \in U_n$, then the set $B_U = \{W_{(i)} : i \in \mathbb{Z}_n^*\}$ is a basis for U_n, and the set $B_V = \{W_{(i)} : i \notin \mathbb{Z}_n^*\}$ is a basis for V_n.*

Proof. Immediate, since B_U and B_V are independent, $B_U \subseteq U_n$ and $B_V \subseteq V_n$, and $U_n = V_n^{\perp}$. ■

Call a matrix *biwrapping* if it is nonsingular and both it and its inverse are wrapping.

THEOREM 1.8. *Let F be a biwrapping matrix, and let a be a vector in $\mathbb{C}^n$. The following three conditions are then equivalent*:

(a) *a is coperiodic,*
(b) *$w(a) = RF$ for some matrix $R \in \mathscr{R}$,*
(c) *$Q^T w(a) = w(a)Q$ for all $Q \in \mathscr{Q}$.*

Proof of Theorem 1.8. Assume first (a), i.e., that $a \in U_n$. Let $v = F^{-1}a$. By the coperiodicity of a the support of v is contained in $\mathbb{Z}_n^*$. Hence, by Corollary 1.6, (b) follows.

Assume next (b). Since F^{-1} is wrapping, it follows from Lemma 1.3 that

$$Q^T F = FQ \tag{3}$$

for all $Q \in \mathscr{Q}$. By (3) and Corollary 1.2 it follows that

$$Q^T w(a) = Q^T RF = RQ^T F = RFQ = w(a)Q,$$

namely, (c).

Finally, assume (c). Taking $Q = Q_k$ in (c), we obtain

$$\sum_{r \in \mathbb{Z}_n : rk = i} a(jr) = \sum_{r \in \mathbb{Z}_n : rk = j} a(ir). \tag{4}$$

Choose in (4) $k = n/d$, $i = 1$, $j = hk$. Then the left hand side of (4) is 0, while the right hand side is equal to the left hand side of (2). This proves that a satisfies Equation (2), i.e., that a is coperiodic. ■

Note that (a) and (c) do not involve the matrix F, yet the above proof of the equivalence between them assumes the existence of a biwrapping matrix F, which is really tantamount to the use of the Fourier transform. Since in this section we wish to avoid such use, we give a proof which does not resort to the existence of a biwrapping matrix:

The implication (c) → (a) has already been proved directly. We need to prove (a) → (c). That is, assuming that a is coperiodic, we have to show (4) for all k, i, and j. Write $K = (k, n)$, $I = (i, n)$, and $J = (j, n)$. Also let $m = n/K$ and $t = k/K$. Then t is invertible modulo m. Let s be such that $st = 1 \bmod m$.

To prove (4) note the following:

(*) $rk = i$ if and only if $K \mid I$ and $rt = i/K \bmod m$, i.e., $r = sI/K \bmod m$.

Case 1: K does not divide I and does not divide J. By (*) the left hand side of (4) is 0, and by the same token the right hand side is also 0.

Case 2: K divides J, but not I. In this case the left hand side of (4) is again 0. Let $u = sj/K$. The right hand side is then equal to $\sum_{f=0}^{n/m-1} a(i(u + mf))$, which, by the coperiodicity of a, is 0. (Notice here that m is a proper divisor of n, since $K \neq 1$, for otherwise $K \mid I$.)

Case 3: K divides I, but not J. This case is symmetrical to case 2.

Case 4: $K \mid I$ and $K \mid J$. By (*) the left hand side of (4) is equal to $\sum\{a(ir): r = sj/K \bmod m\} = \sum_{f=0}^{n/m-1} a(i[sj/K + mf])$. Since $K \mid I$, we have $im = 0 \bmod n$. Hence the last sum is equal to $n/ma(isj/K)$. This expression is symmetric with respect to i and j, and hence a similar calculation yields that the right hand side of (4) is equal to the same number. ∎

We can now prove the result which was the initial goal of our investigation:

THEOREM 1.9. *If $A = w(a)$ is invertible, then A^{-1} is wrapping if and only if a is coperiodic.*

Proof. Assume, first, that A^{-1} is wrapping. By Lemma 1.7 the rows $A^{-1}_{(i)}$, $i \notin \mathbb{Z}_n^*$, of A^{-1} form a basis for V_n. Since a is orthogonal to all of them, it belongs to $V_n^{\perp} = U_n$.

Assume now that $a \in U_n$; then by Theorem 1.8 $Q^TA = AQ$ for all $Q \in \mathcal{Q}$. Hence $A^{-1}Q^T = QA^{-1}$ for all $Q \in \mathcal{Q}$. But this implies, by Lemma 1.3, that A^{-1} is wrapping. ∎

In fact, the above arguments yield a somewhat more general result:

THEOREM 1.10. (a) *The product of an odd number of biwrapping matrices is a biwrapping matrix.*

(b) *The product of an even number of biwrapping matrices belongs to $\mathcal{R}$.*

Proof. By (b) in Theorem 1.8 both parts of the theorem will follow if we prove that the product of two biwrapping matrices belongs to $\mathcal{R}$. Let A, B be biwrapping. By (b) of Theorem 1.8 $A = RF$ for some $R \in \mathcal{R}$, and since F^{-1} is also biwrapping, by the same token $B = SF^{-1}$ for some $S \in \mathcal{R}$. By Lemma 1.1 and Lemma 1.3 it follows that $AB = RFSF^{-1} = RFF^{-1}S^T = RS^T \in \mathcal{R}$. ∎

2. GENERAL ABELIAN GROUPS

In this section we shall generalize the above results from the group $\mathbb{Z}_n$ to general finite abelian groups. The formulation of the results for general abelian groups, as well as the proofs, use the Fourier transform. This approach will enable us to answer a question for which the tools of the previous section did not suffice: when is a wrapping matrix invertible [see Theorem 2.2(b) below]? Necessary background on group representations and Fourier transform on abelian groups can be found, e.g., in [2] and [1].

Let G be a finite abelian group and $\hat{G}$ its character group. Denote by $L(G)$ the linear space of complex valued functions on G. The Fourier transform on G is the linear map $\hat{}: L(G) \to L(\hat{G})$ given by $\hat{f}(\chi) = \sum_{x \in G} \chi(-x) f(x)$. Identifying $\hat{\hat{G}}$ with G by $x(\chi) = \chi(x)$ for $x \in G$, $\chi \in \hat{G}$, it follows that $\hat{\hat{f}}(x) = |G| f(-x)$.

Let m be the maximal order of an element in G, and let $C_m = \{e_m(k) : k \in \mathbb{Z}_m\}$ be the group of mth roots of unity. We shall consider linear maps from $L(G)$ to $L(\hat{G})$ which extend the Fourier transform as follows: For $u \in L(C_m)$ let $S_u : L(G) \to L(\hat{G})$ and $T_u : L(\hat{G}) \to L(G)$ be given by

$$S_u f(\chi) = \sum_{x \in G} u(\chi(-x)) f(x), \qquad T_u g(x) = \sum_{\chi \in \hat{G}} u(\chi(-x)) g(\chi).$$

Thus for $u \equiv 1$, S_u, T_u are the Fourier transforms on $G, \hat{G}$ respectively.

REMARK. The characters of $\mathbb{Z}_n$ are $\chi_i(j) = e_n(ij)$; therefore a wrapping matrix $w(a)$ can be viewed as S_u for $u(e_n(k)) = a(-k)$. Similarly, the inverse of a matrix is wrapping in this case if it can be written as T_v for some $v \in L(\mathbb{Z}_n)$.

The extension of Theorem 1.9 is given in the following two results on the relation between spectral properties of u and the invertibility of S_u.

For $u \in L(C_m)$ let $\mathbf{u} \in L(\mathbb{Z}_m)$ be given by $\mathbf{u}(k) = u(e_m(k))$. The condition of coperiodicity of u which we formulated in $\mathbb{Z}_n$ is given in the present terminology as $\operatorname{Supp} \hat{\mathbf{u}} \subset \mathbb{Z}_m^*$. Thus one direction of Theorem 1.9 is generalized as follows:

THEOREM 2.1. *If S_u is invertible and $S_u^{-1} = T_v$ for some $v \in L(C_m)$, then* $\operatorname{Supp} \hat{\mathbf{u}} \subset \mathbb{Z}_m^*$.

Regard $\mathbb{Z}_m^*$ as a multiplicative group. The characters of $\mathbb{Z}_m^*$ are also called the multiplicative characters of $\mathbb{Z}_m$. For $\eta \in \widehat{\mathbb{Z}_m^*}$ and $k \in \mathbb{Z}_m$ let $G(k, \eta) = \sum_{l \in \mathbb{Z}_m^*} e_m(kl)\eta(l)$ denote the associated Gauss sum.

THEOREM 2.2. *Suppose that* $\operatorname{Supp} \hat{\mathbf{u}} \subset \mathbb{Z}_m^*$. *Then*:

(a) *If* S_u *is invertible then* $S_u^{-1} = T_v$ *for some* $v \in L(C_m)$.

(b) S_u *is invertible if and only if there exists a function* $c : \widehat{\mathbb{Z}_m^*} \to \mathbb{C}^*$ *such that* $\mathbf{u}(k) = \sum_{\eta \in \widehat{\mathbb{Z}_m^*}} c(\eta) G(k, \eta)$ *for all* $k \in \mathbb{Z}_m$.

Proof of Theorem 2.1. If $u, v \in L(C_m)$ satisfy $T_v S_u = I$, then for all $x, y \in G$

$$\sum_{\chi \in \hat{G}} u(\chi(x)) v(\chi(y)) = \delta(x, y). \tag{5}$$

For $y \in G$ define $v_y \in L(\hat{G})$ by $v_y(\chi) = v(\chi(y))$. Let $\langle y \rangle$ denote the subgroup generated by y.

CLAIM. *If* $x \notin \langle y \rangle$ *then* $\widehat{v_y}(x) = 0$.

Proof.

$$\widehat{v_y}(x) = \sum_{\chi \in \hat{G}} \chi(-x) v(\chi(y)) = \sum_{\omega \in C_m} v(\omega) \sum_{\{\chi : \chi(y) = \omega\}} \chi(-x).$$

Now $x \notin \langle y \rangle$ implies that all inner sums are 0. ∎

Equation (5) implies that $\{v_y : y \in G\}$ are linearly independent in $L(\hat{G})$ and therefore $\{\widehat{v_y} : y \in G\}$ are linearly independent in $L(G)$. Since $u(\chi(x)) = (1/m) \sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k) \chi(kx)$, it follows that

$$\begin{aligned}
\sum_{\chi \in \hat{G}} u(\chi(x)) v(\chi(y)) &= \sum_{\chi \in \hat{G}} u(\chi(x)) v_y(\chi) \\
&= \frac{1}{m} \sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k) \sum_{\chi \in \hat{G}} \chi(kx) v_y(\chi) \\
&= \frac{1}{m} \sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k) \widehat{v_y}(-kx).
\end{aligned} \tag{6}$$

Let $x_0 \in G$ be an element of the maximal order m, and let

$$A = \{y \in G : \langle y \rangle \subsetneqq \langle x_0 \rangle\}.$$

Then $|A| = m - \phi(m)$, where $\phi(m)$ is Euler's function. Let $W = \operatorname{Span}\{\widehat{v_y} : y \in A\} \subset L(G)$. Then by the Claim, $\operatorname{Supp} w \subset A$ for all $w \in W$. Together with $\dim W = |A|$, this implies that $W = \{w \in L(G) : \operatorname{Supp} w \subset A\}$. In particular, for all $l \notin \mathbb{Z}_m^*$, W contains the function $w_l(x) = \delta(x, -lx_0)$.

Now (5) and (6) imply that for all $w \in W$

$$\sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k) w(-kx_0) = 0. \tag{7}$$

Applying (7) with $w = w_l$ for $l \notin \mathbb{Z}_m^*$, it follows that $\operatorname{Supp} \hat{\mathbf{u}} \subset \mathbb{Z}_m^*$. ∎

Proof of Theorem 2.2. For $k \in \mathbb{Z}_m^*$ let $\sigma_k : G \to G$ be given by $\sigma_k(x) = kx$. (This corresponds to Q_k in Section 1.) σ_k acts on $L(G)$ by $\sigma_k f(x) = f(\sigma_k^{-1} x)$. In particular σ_k acts on $\hat{G} \subset L(G)$ and hence also on $L(\hat{G})$.

Let H be the group $\{\sigma_k : k \in \mathbb{Z}_m^*\}$, where $\sigma_k \sigma_l = \sigma_{kl}$, and let $C[H]$ denote the group algebra of H. The actions of $C[H]$ on $L(G)$ and $L(\hat{G})$ commute with the Fourier transform $\tau\hat{f} = \widehat{\tau f}$ for all $\tau \in C[H]$, $f \in L(G)$.

Suppose now that $u \in L(C_m)$ satisfies $\operatorname{Supp} \hat{\mathbf{u}} \subset \mathbb{Z}_m^*$. Then for $f \in L(G)$

$$S_u f(\chi) = \sum_{x \in G} u(\chi(-x)) f(x) = \frac{1}{m} \sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k) \sum_{x \in G} \chi(-\sigma_k x) f(x)$$

$$= \frac{1}{m} \sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k) \sum_{x \in G} \chi(-x) \sigma_k f(x) = \frac{1}{m} \sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k) \widehat{\sigma_k f}(\chi).$$

Denoting $Q_u = (1/m)\sum_{k \in \mathbb{Z}_m} \hat{\mathbf{u}}(k)\sigma_k \in C[H]$, it then follows that $S_u f(\chi) = \widehat{Q_u f}(\chi)$ for all $f \in L(G)$. Similarly, if $R_v = (1/m)\sum_{k \in \mathbb{Z}_m} \hat{\mathbf{v}}(k^{-1})\sigma_k \in C[H]$ then $T_v g(x) = \widehat{R_v g}(x)$ for all $g \in L(\hat{G})$.

It follows that S_u is invertible if and only if Q_u is invertible as an operator on $L(G)$. Since $C[H]$ acts faithfully on $L(G)$, this in turn is equivalent to the invertibility of Q_u in $C[H]$.

To prove (a) note that $\hat{}\cdot\hat{=}|G|\sigma_{-1}$ and so

$$S_u^{-1} = \left(\hat{}\cdot Q_u\right)^{-1} = Q_u^{-1}\cdot\left(|G|^{-1\hat{}}\cdot\sigma_{-1}\right) = \hat{}\cdot\left(|G|^{-1}Q_u^{-1}\cdot\sigma_{-1}\right).$$

Therefore $S_u^{-1} = T_v$, where v satisfies $R_v = |G|^{-1}Q_u^{-1}\sigma_{-1}$. The vector v may be written explicitly as follows: if $Q_u^{-1} = \sum_{k\in\mathbb{Z}_m^*} b_k\sigma_k \in C[H]$, then v is given by $v(\omega) = |G|^{-1}\sum_{l\in\mathbb{Z}_m^*} b_l\omega^{-l^{-1}}$ for all $\omega \in C_m$.

To prove (b) let $a_k = (1/m)\hat{\mathbf{u}}(k)$. Then $Q_u = \sum_{k\in\mathbb{Z}_m^*} a_k\sigma_k$ is invertible in $C[H]$ if and only if $c'(\eta) = \sum_{k\in\mathbb{Z}_m^*} a_k\eta(k) \neq 0$ for all $\eta \in \widehat{\mathbb{Z}_m^*}$.

To express $\mathbf{u}$ in terms of c', we first apply Fourier inversion on $\mathbb{Z}_m^*$ to obtain

$$\frac{1}{m}\hat{\mathbf{u}}(k) = a_k = \frac{1}{\phi(m)}\sum_{\eta\in\widehat{\mathbb{Z}_m^*}} c'(\eta)\eta(k^{-1}),$$

and then Fourier inversion on $\mathbb{Z}_m$, which finally gives

$$\mathbf{u}(k) = \frac{1}{m}\sum_{l\in\mathbb{Z}_m}\hat{\mathbf{u}}(l)e_m(lk) = \frac{1}{\phi(m)}\sum_{l\in\mathbb{Z}_m^*}\left(\sum_{\eta\in\widehat{\mathbb{Z}_m^*}} c'(\eta)\eta(l^{-1})\right)e_m(lk)$$

$$= \frac{1}{\phi(m)}\sum_{\eta\in\widehat{\mathbb{Z}_m^*}} c'(\eta)\sum_{l\in\mathbb{Z}_m^*} e_m(lk)\eta(l^{-1}) = \sum_{\eta\in\widehat{\mathbb{Z}_m^*}}\frac{c'(\eta^{-1})}{\phi(m)}G(k,\eta).$$

■

REFERENCES

1 M. Naimark and D. Stern, *Theory of Group Representations*, Springer-Verlag, New York, 1982.

2 J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.

3 P. Diaconis, Patterned matrices, in *Matrix Theory and Applications*, Proc. AMS Symp. Appl. Math. 40 (C. Johnson, Ed.), 1989.

Received 30 April 1995; final manuscript accepted 6 January 1996